Notice of Allowability	Application No.	Applicant(s)	
	09/893,785	OHKUMA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment received 16 January 2007*.

2. ☒ The allowed claim(s) is/are *1,4,8-13 and 16*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

1. An amendment was received on 16 January 2007. By this amendment, Claims 1, 4, and 8-18 have been amended. Claims 5 and 6 have been canceled. No new claims have been added. Claims 1, 4, and 8-18 are currently pending in the present application.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joe Wrkich on 26 March 2007.

3. The application has been amended as follows:

IN THE CLAIMS:

Please **CANCEL Claims 14, 15, 17, and 18**.

Allowable Subject Matter

4. Claims 1, 4, 8-13, and 16 are allowed.

5. The following is an examiner's statement of reasons for allowance:

Independent Claim 1 is directed to an apparatus for block encryption, and independent Claim 16 is directed to a corresponding apparatus for decryption. Each includes a series of encrypting (or decrypting) sections with each section including randomizing units and a diffusing unit. The randomizing units further include an additional diffusing subunit and randomizing subunits both before ("first subunits") and after ("third subunits") the diffusing subunit. The first randomizing subunits in one section are connected to the first randomizing subunits in the next encrypting (or decrypting) section in the series by multiple (i.e. at least two) paths. Independent Claim 4 is directed to a block encryption apparatus that corresponds substantially to the apparatus of Claim 1. Independent Claims 12 and 13 are also directed to block encryption apparatus similar to those of Claim 4, and further specifying particular block sizes and operations performed on matrices over a Galois field $GF(2^4)$. All of the independent Claims recite a limitation corresponding to that recited in Claim 1, where units corresponding to the first randomizing subunits (i.e. second nonlinear transformation units as recited in independent Claims 4, 12, and 13) are connected to the corresponding units in the next encrypting section in the series by multiple (i.e. at least two) paths.

The closest prior art, Delayaye et al, US Patent 4751733, *inter alia*, discloses block ciphers using a substitution permutation network, where substitution corresponds to the claimed randomizing or nonlinear transformation units, and permutation corresponds to the diffusing units. However, Delayaye does not teach or suggest that the substitution units are connected to subsequent substitution units by multiple paths. Okhuma et al, "The block cipher Hierocrypt", cited by Applicant in the information disclosure statement received 29 June 2001, discloses the substitution permutation network but does not teach or suggest the multiple path connection requirement. Okhuma et al, "Security and Performance Evaluations for the block ciphers Hierocrypt-3 and Hierocrypt-L1", also cited by Applicant in the information disclosure statement received 29 June 2001, discloses block ciphers having a substation permutation network and discloses the multiple path requirement (see page 75, section 3.2.3) but was not published prior to the foreign priority date of the present application. Therefore, the claims are allowable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Muratani et al, US Patent 7194090, discloses a nested SPN block cipher, but does not disclose the requirement of multiple paths.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER